UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,876	04/16/2004	Keisuke Yamaguchi	SCEP 21.113 (100809-00239	1439

26304 7590 03/31/2008

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
03/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/826,876	YAMAGUCHI ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/4/04; 8/29/05; 7/18/06; 9/28/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. ***Claims 12 and 16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.***

Claims 12 and 16 recites a computer program which makes a computer carry out functions. These claims are directed to a program and instructions. Thus, are purely program per se because the claimed program and functions are not embodied on a tangible medium.

> ***MPEP: 2106.01 [R-5] -*** *I. FUNCTIONAL DESCRIPTIVE MATERIAL: "DATA STRUCTURES" REPRESENTING DESCRIPTIVE MATERIAL PER SE OR COMPUTER PROGRAMS REPRESENTING COMPUTER LISTINGS PER SE*
>
> Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g.,Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory.
>
> Similarly, computer programs claimed as computer listings per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. *Claims 1-5 and 9 recite the limitation* "own terminal" ***in*** a request unit. ***There is insufficient antecedent basis for this limitation in the claim.***

Claims 1 and 9 recites "a registration request unit which sends the certificate to the management server, to make a request for registration of the network address, which is assigned to the own terminal, the authentication server comprising". Claims 1 and 9 recites "the terminal" but "the own terminal" was not recited previously. Thus, it is unclear whether the terminal and the own terminal are different terminals or one in the same which then suggests it is a grammatical error.

All dependent claims are also rejected by virtue of their pendency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. *Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Donley, et al. (US 7,190,948), and further in view of Hind, et al. (US 6,823,454).*

As per claim 1:

Donley discloses a communication management system comprising:

a terminal of a user; (col.4, lines 42-60; *subscriber is the user and terminal given as communication device of the subscriber.*)

an authentication server which authenticates the terminal; and (col.3, lines 59-60)

a management server which manages network address which uniquely identifies the terminal on a network (col.8, lines 23-33), the terminal comprising:

a holding unit which holds a device ID which is specifically assigned to the terminal in such a manner as to uniquely identify the terminal; (col.8, lines 19-23; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

an authentication request unit which reads the device ID from the holding unit, and

sends the device ID to the authentication server to make a request for authentication;

(col.8, lines 14-18)

a certificate acquisition unit which acquires a certificate, which certifies success in the authentication, from the authentication server; and (col.2, lines 64-67 and col.7, lines 13-16)

a registration request unit which sends the certificate to the management server, *[to make a request for registration of the network address*], which is assigned to the own terminal (col.8, lines 30-54), the authentication server comprising:

an authentication reception unit which acquires the device ID from the terminal and receives the request for the authentication; (col.3, lines 59-60 and col.6, lines 31-35 and 43-44)

an authentication unit which authenticates the correctness of the device ID of the terminal; and (col.6, lines 44-49)

a certificate issue unit which issues a certificate when succeeding in the authentication of the terminal (col.3, lines 46-50), the management server comprising:

a database which holds an ID which uniquely identifies the terminal, and the network address in a manner that they are associated with each other; (col.6, lines 43-50)

a registration reception unit which acquires the certificate from the terminal, and *[receives the request for registration of the network address of the terminal]*; (col.7, lines 8-11)

a registration unit which verifies the correctness of the certificate, and *[registers the ID and the network address of the terminal in the database when the certificate is confirmed to be correct];* (col.7, lines 13-16)

[an inquiry reception unit which receives the request for inquiring the network address of the terminal;]

a search unit which searches through the database on the basis of the ID of the terminal as the target of an inquiry, to acquire the network address of the terminal; and (col.8, lines 12-40)

an answer unit which answers search result. (col.8, lines 37-54)

Although Donley discloses the terminal, authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of the request for registration of the network address of the terminal and registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a

stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as legitimate before responding with an associated address, thus, protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

As per claim 2: See Hind - col.3, lines 1-6; discussing a communication management system according to claim 1, wherein the holding unit holds the device ID in such a manner that the device ID is un-rewritable from outside.

As per claim 3: See Donley - col.6, lines 31-35 and Hind - col.11, lines 56-67 and col.12, lines 15-42; discussing a communication management system according to claim 1, wherein the authentication server further comprises an ID issue unit which issues an ID for uniquely identifying the terminal when succeeding in authentication of the terminal, wherein the registration reception unit receives the ID from the terminal, the ID being issued by the ID issue unit to the terminal, and the registration unit registers the ID, issued by the ID issue unit to the terminal, and the network address in the database.

As per claim 4: See Donley - col.8, lines 7-25; discussing the communication management system according to claim 1, wherein the management server further comprises a group database which holds information related to a group including a plurality of the terminals, wherein the inquiry reception unit receives a request for an inquiry about the group, and the search unit searches through the group database on the basis of the request for the inquiry.

As per claim 5: See Donley - col.8, lines 12-54 and Hind - col.11, lines 17-30 and col.12, lines 15-42; discussing the communication management system according to claim 1, wherein the management server further comprises a matching control unit which controls matching of a communication partner between the terminals, wherein the inquiry reception unit receives a requirement for the communication partner, and the search unit searches through the database on the basis of the requirement, and the matching control unit determines the communication partner on the basis of search result, and the answer unit answers the communication partner.

As per claim 6:

Donley discloses a method for managing communication comprising:

reading a device ID by a terminal of a user, the device ID unique to the terminal being held in a memory in the terminal; (col.6, lines 31-35; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

sending the device ID from the terminal to an authentication server for authenticating the terminal; (col.8, lines 14-18; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

authenticating the correctness of the device ID by the authentication server; (col.6, lines 44-49)

issuing a certificate for certifying success in authentication by the authentication server, when succeeding in the authentication; (col.3, lines 46-50 and col.7, lines 8-11)

sending the certificate from the authentication server to the terminal; (col.7, lines 8-16)

sending the certificate from the terminal to a management server, the management server managing a network address for uniquely identifying the terminal on a network; (col.8, lines 12-40)

verifying the certificate by the management server; and *[storing an ID for uniquely identifying the terminal and the network address in a database by the management server, in a manner that they are associated with each other, when the certificate is confirmed to be correct].* (col.8, lines 37-54).

Although Donley discloses the terminal, Authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of storing an ID for uniquely identifying the terminal and the network address

in a database by the management server, in a manner that they are associated with each other, when the certificate is confirmed to be correct.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach storing an ID for uniquely identifying the terminal and the network address in a database by the management server, in a manner that they are associated with each other, when the certificate is confirmed to be correct because this validates the requester that the identity is verified as legitimate before responding with an associated address, thus,

protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

As per claim 7: See Hind - col.3, lines 42-53 and col.12, lines 15-42; discussing the method according to claim 6, wherein steps from reading the device ID to storing in the database are automatically carried out without involvement by a user.

As per claim 8: See Hind - col.9, lines 50-67 and col.11, lines 17-30 and col.12, lines 15-42; discussing the method according to claim 6 further comprising: receiving a request for an inquiry about the network address of the terminal by the management server; searching through the database on the basis of the ID of the terminal by the management server, to acquire the network address of the terminal; and answering the network address by the management server.

As per claim 9:

Donley discloses a terminal device comprising:

a holding unit which holds a specific device ID, the device ID being assigned so as to uniquely identify the terminal device itself; (col.3, lines 59-60 and col.6, lines 31-35 and 43-44; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

an authentication request unit which reads the device ID from the holding unit, and sends the device ID to an authentication server which authenticates the terminal, to make a request for authentication; (col.8, lines 14-18; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

a certificate acquisition unit which acquires a certificate, which certifies success in the authentication, from the authentication server; and (col.6, lines 31-49 and col.7, lines 8-11)

a registration request unit which sends the certificate to a management server which manages a network address for uniquely identifying the terminal device on a network (col.8, lines 12-40), *[to make a request for registration of the network address assigned to the own terminal device].* (col.8, lines 37-54)

Although Donley discloses the terminal, Authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of the request for registration of the network address assigned to the terminal.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as legitimate before responding with an associated address, thus, protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

As per claim 10:

Donley discloses a method for managing communication comprising:

reading a specific device ID from a memory, the device ID being assigned so as to uniquely identify a terminal; (col.6, lines 31-35; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

sending the device ID to an authentication server which authenticates the terminal, to make a request for authentication; (col.8, lines 14-18; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

acquiring a certificate, which certifies success in the authentication, from the authentication server; and (col.6, lines 31-49 and col.7, lines 8-11)

sending the certificate to a management server which manages a network address for uniquely identifying the terminal on a network (col.7, lines 8-13 and col.8, lines 12-40), in order to *[make a request for registration of the network address assigned to the terminal].*
(col.8, lines 37-54)

Although Donley discloses the terminal, Authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of the request for registration of the network address assigned to the terminal.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as

legitimate before responding with an associated address, thus, protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

11. The method according to claim 10, further comprising, prior to the step of sending the certificate to make the request for registration: making a request of a connection server for mediating connection to the network to connect the terminal to the network; and acquiring the network address assigned by the connection server to the terminal, wherein, in the step of sending the certificate to make the request for registration, registration of the network address assigned by the connection server is required.

As per claim 12:

Donley discloses a computer program which makes a computer carry out:

a function of reading a specific device ID from a memory, the device ID being assigned so as to uniquely identify a terminal; (col.3, lines 59-60 and col.6, lines 31-35 and 43-44; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

a function of sending the device ID to an authentication server which authenticates the terminal, to make a request for authentication; (col.8, lines 14-18; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

a function of acquiring a certificate, which certifies success in the authentication, from the authentication server; and (col.6, lines 31-49 and col.7, lines 8-11)

a function of sending the certificate to a management server which manages a network address for uniquely identifying the terminal on a network (col.7, lines 8-13 and col.8, lines 12-

40), in order to *[make a request for registration of the network address assigned to the terminal].* (col.8, lines 37-54)

Although Donley discloses the terminal, Authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of the request for registration of the network address assigned to the terminal.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database

when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as legitimate before responding with an associated address, thus, protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

As per claim 13:

Donley discloses a computer-readable recording medium which stores a program to make a computer carry out:

a function of reading a specific device ID from a memory, the device ID being assigned so as to uniquely identify a terminal; (col.3, lines 59-60 and col.6, lines 31-35 and 43-44; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

a function of sending the device ID to an authentication server which authenticates the terminal, to make a request for authentication; (col.8, lines 14-18; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

a function of acquiring a certificate, which certifies success in the authentication, from the authentication server; and (col.6, lines 31-49 and col.7, lines 8-11)

a function of sending the certificate to a management server which manages a network address for uniquely identifying the terminal on a network (col.7, lines 8-13 and col.8, lines 12-40), in order to *[make a request for registration of the network address assigned to the terminal].* (col.8, lines 37-54)

Although Donley discloses the terminal, Authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of the request for registration of the network address assigned to the terminal.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as

legitimate before responding with an associated address, thus, protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

As per claim 14:

Donley discloses a management server comprising:

a database which holds an ID for uniquely identifying a terminal and a network address of the terminal in a manner that they are associated with each other; (col.8, lines 19-30; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

a registration reception unit which acquires a certificate from the terminal and *[receiving a request for registering a network address of the terminal]*, the certificate being issued by an authentication server which authenticates the terminal to certify success in authentication of the terminal;

a registration unit which verifies the correctness of the certificate, and *[registers the ID and the network address of the terminal in the database, when the certificate is confirmed to be correct]*;

an inquiry reception unit which receives a request for an inquiry about the network address of the terminal; (col.8, lines 12-18; *device ID is given as credentials associated with the subscriber where it includes unique user/ subscriber identifier (col.6, lines 31-35 and 43-44).*)

a search unit which searches through the database on the basis of the ID of the terminal as the target of the inquiry, to acquire the network address of the terminal; and (col.8, lines 19-40)

an answer unit which answers search result. (col.8, lines 37-54)

Although Donley discloses the terminal, authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of the request for registration of the network address of the terminal and registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database

when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as legitimate before responding with an associated address, thus, protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

As per claim 15:

Donley discloses a method for managing communication comprising:

acquiring a certificate from a terminal, and *[receiving a request for registering a network address of the terminal]*, the certificate being issued by an authentication server which authenticates the terminal to certify success in authentication of the terminal; (col.8, lines 19-30; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

verifying the correctness of the certificate, and *[registering an ID for uniquely identifying the terminal and the network address of the terminal in a database, when the certificate is confirmed to be correct]*;

receiving a request for an inquiry about the network address of the terminal; (col.8, lines 13-18; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

searching through the database on the basis of the ID of the terminal as the target of the inquiry, to acquire the network address of the terminal; and (col.8, lines 19-40)

answering search result. (col.8, lines 37-54)

Although Donley discloses the terminal, Authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did

not go into details of the request for registration of the network address of the terminal and registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as

legitimate before responding with an associated address, thus, protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

As per claim 16:

Donley discloses a computer program which makes a computer carry out:

a function of acquiring a certificate from a terminal, and *[receiving a request for registering a network address of the terminal]*, the certificate being issued by an authentication server which authenticates the terminal to certify success in authentication of the terminal; (col.8, lines 19-30; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

a function of verifying the correctness of the certificate, and *[registering an ID for uniquely identifying the terminal and the network address of the terminal in a database, when the certificate is confirmed to be correct]*;

a function of receiving a request for an inquiry about the network address of the terminal; (col.8, lines 13-18; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

a function of searching through the database on the basis of the ID of the terminal as the target of the inquiry, to acquire the network address of the terminal; and (col.8, lines 19-40)

a function of answering search result. (col.8, lines 37-54)

Although Donley discloses the terminal, Authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of the request for registration of the network address of the terminal and

registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as legitimate before responding with an associated address, thus, protects from tampering or

hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

As per claim 17:

Donley discloses a computer-readable recording medium which stores a program to make a computer carry out:

a function of acquiring a certificate from a terminal, and *[receiving a request for registering a network address of the terminal]*, the certificate being issued by an authentication server which authenticates the terminal to certify success in authentication of the terminal; (col.8, lines 19-30; *subscriber is the user and terminal given as communication device of the* subscriber (col.4, lines 42-60).)

a function of verifying the correctness of the certificate, and *[registering an ID for uniquely identifying the terminal and the network address of the terminal in a database, when the certificate is confirmed to be correct]*;

a function of receiving a request for an inquiry about the network address of the terminal; (col.8, lines 13-18; *device ID is given as credentials associated with the subscriber where it includes unique user/subscriber identifier (col.6, lines 31-35 and 43-44).*)

a function of searching through the database on the basis of the ID of the terminal as the target of the inquiry, to acquire the network address of the terminal; and (col.8, lines 19-40)

a function of answering search result. (col.8, lines 37-54)

Although Donley discloses the terminal, Authentication server, and certificate server wherein the device ID identifies the terminal and its associated address. However, Donley did not go into details of the request for registration of the network address of the terminal and

registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct.

Hind discloses an invention for using device certificates to authenticate serves before automatic address assignment (col.1, lines 14-18). Hind discusses a DNS server maintains a stored mapping of host names to IP addresses. Upon receiving a query for a particular host name, the DNS server can return the stored IP address mapped to the associated host name (col.1, lines 35-38). This suggests the ID and network address are associated with each other and are registered. Hind the server requesting an assigned address is authenticated before assigning an address thereto so that the source of the automatically assigned address can be authenticated before the address is used by the server (col.3, lines 42-53 and col.12, lines 15-42). Hind discusses receiving an address assignment response, authenticating the device and returning the address response to the server device (col.4, lines 11-24). Hind uses a serial number or other identifier is used as a unique identifier that will authenticate the device (col.11, lines 56-67). Authentication at the physical level makes it much more difficult to compromise the security of the device (col.9, lines 50-67) and validates the requester is authentic before obtaining and returning the requested address (col.14, lines 30-60). Thus, Hind's invention provides protection from tampering and hacking (col.3, lines 15-37).

Therefore, it would have been obvious for a person ordinary skills in the art to combine Donley with Hind to teach registers the ID and network address of the terminal in the database when the certificate is confirmed to be correct with the request for registration of the network address of the terminal because this validates the requester that the identity is verified as

legitimate before responding with an associated address, thus, protects from tampering or hacking (Hind - col.3, lines 14-37 and col.9, lines 50-67 and col.14, lines 30-60).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135